UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/091,479	03/07/2002	Eric Rescorla	730.39867X00	3321

22907 7590 08/17/2006

BANNER & WITCOFF
1001 G STREET N W
SUITE 1100
WASHINGTON, DC 20001

EXAMINER	
WON, MICHAEL YOUNG	
ART UNIT	**PAPER NUMBER**
2155	

DATE MAILED: 08/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/091,479	RESCORLA ET AL.	
	Examiner	Art Unit	
	Michael Y. Won	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-31 and 34-65* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28-31 and 34-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment and Request for Continued Examination filed May 30, 2006.

2. Claims 28, 30, 43, 44, and 46-49 have been amended and claims 32 and 33 have been cancelled.

3. New claims 55-65 have been added.

4. Claims 28-31 and 34-65 have been examined and are pending with this action.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 28, 44, 46, 49, 55, and 62 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Although on page 11, lines 26-27 of the specification states, that the "clustering state information" **may** occur **after** receiving an acknowledgment, the examiner could not find conclusive evidence that would suggest that the "clustering state information" occurs "**in response to** receiving an acknowledgment" as recited in claims 28 and 46 (emphasis added), "**in response to** receiving a client handshake" as recited in claim 44 (emphasis added), and "**only in response** to an acknowledgment" as recited in claims 49 (emphasis added). These limitations claim that the occurrence of an action (i.e. receiving an acknowledgment, client handshake, acknowledgement, respectively) triggers another action (i.e. clustering state information). Such explicit teachings are not supported by the specification.

Furthermore, the examiner could not find any teachings within the specification of "receiving an acknowledgement from the second node in response to determining that the transferred information is a full record" as recited in claim 28 and similarly recited in claims 46 and 49. Page 16, lines 20-21 states, "When a full record has been ACKed, it may be removed from the list and a new state clustered". Such teachings does not suggest, "**determining** that the transferred information is a full record" much less "receiving an acknowledgement from the second node in **response to** determining that the transferred information is a full record" (emphasis added).

Lastly there is no support in the specification of "clustering the transferred information **in response to** determining that the transferred information is a partial record" and "transmitting a partial acknowledgement to the first node **upon** clustering the transferred information" as recited in claims 55 and 62 (emphasis added).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 28-31, 34-36, 39-40, 42- 57, and 60-64 are rejected under 35 U.S.C. 102(e) as being anticipated by Bruck et al. (US 6,691,165 B1).

INDEPENDENT:

As per ***claim 28***, Bruck teaches a method for clustered Secure Sockets Layer (SSL) acceleration comprising the steps of:

connecting at least two SSL (see col.27, lines 55-65: "*secure socket layer (SSL) network communication connection*") relays in a cluster (see Fig.2, #200; Fig.17, #1704; col.5, lines 33-35 & 38-40: "*The front-layer servers 200 will also be referred to as a server cluster or gateway*"; and col.28, lines 17-20: "*distributed server 1703 of a server cluster 1704*");

establishing a communication path between a first node and a second node via a first SSL relay of the cluster (see Fig.2; Fig.17; col.2, lines 63-65: "*communication*

between clients and servers"; and col.25, lines 64-col.26, line 2: "*connection between two machines are established*");

transferring information between the first node and the first SSL relay, the transferred information related to a communication from the first node to the second node (see col.6, lines 22-33 and col.27, lines 1-11: "*each distributed gateway of the cluster receives traffic*");

transferring the information between the first SSL relay and the second node (see col.3, lines 18-21 and col.28, lines 20-23);

receiving an acknowledgment from the second node in response to determining that the transferred information is a full record (see col.24, lines 40-66: "*after all packets have been acknowledged by the receiver*"); and

clustering state information of the communication path (see col.10, lines 9-18: "*provides state sharing information among the all the machines in the cluster*"; and col.24, lines 31-33: "*Consistent state sharing among the servers in the cluster is important for the distributed server application in accordance with the invention*" & lines 40-42: "*The foundation of the Consistent State Sharing mechanism is a Reliable Message layer that is implemented...* ") in response to receiving an acknowledgment from the second node (see col.24, lines 45-47: "*if the Reliable Message layer still fails to receive acknowledgment ...* "), the clustering comprising sharing the state information between the first SSL relay and at least a second SSL relay of the relay cluster (see col.10, lines 9-18: "*provides state sharing information among the all the machines in the cluster*"), wherein the second SSL relay is capable of taking over the communication

between the first and second node upon failure of the first SSL relay (see col.2, lines 49-54: "*when a server failure at either layer is detected, the system automatically shifts network traffic from the failed machine to one or more operational machines*"; col.3, lines 37-44; and col.7, lines 45-49: "*fail-over capability*").

As per ***claim 44***, Bruck teaches a system for clustered Secure Sockets Layer (SSL) acceleration comprising:

a first node (see col.5, line 55: "*client*");

a second node (see col.5, lines 36-38: "*back-end servers... application servers*" & 55: "*servers*"); and

an SSL (see col.27, lines 55-65: "*secure socket layer (SSL) network communication connection*") relay cluster (see Fig.2, #200; Fig.17, #1704; col.5, lines 33-35 & 38-40: "*The front-layer servers 200 will also be referred to as a server cluster or gateway*"; and col.28, lines 17-20: "*distributed server 1703 of a server cluster 1704*") for connecting the first node and the second node (see Fig.2 and Fig.17) comprising:

a first SSL relay configured to cluster state information (see col.10, lines 9-18: "*provides state sharing information among the all the machines in the cluster*"; and col.24, lines 31-33: "*Consistent state sharing among the servers in the cluster is important for the distributed server application in accordance with the invention*" & lines 40-42: "*The foundation of the Consistent State Sharing mechanism is a Reliable Message layer that is implemented...* ") in response to receiving a client handshake from the first node (see col.24, lines 45-47: "*if the*

Reliable Message layer still fails to receive acknowledgment ... " and col.25, line 64-col.26, line 2: "connection between two machines are established following an exchange of messages including a synchronization segment message (SYN), acknowledgement message (ACK), and SYN-acknowledgement message (SYN-ACK)"); and

a second SSL relay configured to transmit an acknowledgement to the first SSL relay upon receiving the state information (see col.8, lines 45-52: "*tracks acknowledgement messages communicated around the server cluster*" and col.10, lines 14-18: "*state-sharing protocol word is passed around the cluster machines... in a token ring arrangement*"),

wherein the first SSL relay is further configured to transmit a handshake acknowledgement message to the first node upon receiving the acknowledgement from the second SSL relay (see col.25, line 1-3: "*On the receiver side of the Reliable Message layer processing, for every packet received, the Reliable Message layer send out an acknowledgement*").

As per ***claim 46***, Bruck teaches computer readable medium storing computer readable instructions that, when executed by a processor, performs a method comprising:

establishing a connection between a first node and a second node via a first SSL (see col.27, lines 55-65: "*secure socket layer (SSL) network communication connection*") relay of an SSL relay cluster (see Fig.2, #200; Fig.17, #1704; col.5, lines

33-35 & 38-40: "*The front-layer servers 200 will also be referred to as a server cluster or gateway*"; and col.28, lines 17-20: "*distributed server 1703 of a server cluster 1704*"), wherein said SSL relay cluster comprises at least two interconnected SSL relays cluster (see Fig.2; Fig.17; and col.2, lines 63-65: "*communication between clients and servers*");

receiving a data communication from the first node (see col.6, lines 22-33 and col.27, lines 1-11: "*each distributed gateway of the cluster receives traffic*");

transmitting the data communication to the second node (see col.3, lines 18-21 and col.28, lines 20-23);

receiving a first acknowledgment from the second node in response to a determination that the transmitted data communication is a full record (see col.24, lines 40-66: "*after all packets have been acknowledged by the receiver*");

in response to the first acknowledgment (see col.8, lines 45-52: "*tracks acknowledgement messages communicated around the server cluster*"), clustering state information of the established connection with at least a second SSL relay of the SSL relay cluster (see col.6, lines 4-7: "*state sharing*"; col.10, lines 9-18: "*provides state sharing information among the all the machines in the cluster*"; and col.25, lines 27-32); and

receiving a second acknowledgment from the at least second SSL relay in the SSL relay cluster confirming successful clustering (see col.8, lines 45-52: "*tracks acknowledgement messages communicated around the server cluster*" and col.10, lines

14-18: "*state-sharing protocol word is passed around the cluster machines... in a token ring arrangement*").

As per ***claim 49***, Bruck teaches an SSL relay, the SSL relay connected in a cluster of SSL relays, comprising:

a first interface (see Fig.3; col.6, line 65-col.7, line 7; and col.7, lines 16-21) for transferring information between a first node and the SSL relay (see col.6, lines 22-33 and col.27, lines 1-11: "*each distributed gateway of the cluster receives traffic*");

a second interface (see Fig.3; col.6, line 65-col.7, line 7; and col.7, lines 16-21) for transferring information between a second node and the SSL relay (see col.3, lines 18-21 and col.28, lines 20-23);

a third interface (see Fig.3; col.6, line 65-col.7, line 7; and col.7, lines 16-21) for transferring state information (see col.6, lines 4-7: "*state sharing*"; col.10, lines 9-18: "*provides state sharing information among the all the machines in the cluster*"; and col.25, lines 27-32) between SSL (see col.27, lines 55-65: "*secure socket layer (SSL) network communication connection*") relays in the cluster (see Fig.2, #200; Fig.17, #1704; col.5, lines 33-35 & 38-40: "*The front-layer servers 200 will also be referred to as a server cluster or gateway*"; and col.28, lines 17-20: "*distributed server 1703 of a server cluster 1704*") only in response to an acknowledgment from the second node (see col.8, lines 45-52: "*tracks acknowledgement messages communicated around the server cluster*"), wherein the acknowledgement is received in response to a

determination that the transferred information is a full record (see col.24, lines 40-66: "*after all packets have been acknowledged by the receiver*"); and

a storage device, wherein state information of an SSL connection between the first node and the SSL relay is shared across each SSL relay in the cluster any of the SSL relays in the cluster capable of taking over all connections of another SSL relay in the cluster (see col.8, lines 45-52: "*tracks acknowledgement messages communicated around the server cluster*" and col.10, lines 14-18: "*state-sharing protocol word is passed around the cluster machines... in a token ring arrangement*"), wherein the storage device is further configured to store the transferred information in a queue until acknowledgment is received form the second node (see col.32, lines 34-36: "cache the assignment data").

DEPENDENT:

As per ***claims 29, 45, 48, and 50***, which depend on claims 28, 44, 46, 49, respectively, Bruck further teaches wherein the first node comprises a client and the second node comprises a server (see col.2, lines 63-65).

As per ***claim 30***, which depends on claim 28, Bruck teaches of further comprising transferring information associated with communications between the first node and a second to the second SSL relay transparently upon failure of the first SSL relay (see col.2, lines 49-54 & 63-65 and col.8, lines 62-65).

As per ***claim 31***, which depends on claim 28, Bruck teaches of further comprising transmitting the communication from the first node to a second SSL relay

and from the second SSL relay to the second node transparently upon failure of the first SSL relay (see claim 28 and 30 rejections above).

As per ***claim 34***, which depends on claim 28, Bruck teaches of further comprising sharing an SSL session cache across all of the at least two SSL relays (see col.16, line 66-col.17, line 6).

As per ***claim 35***, which depends on claim 28, Bruck teaches of further comprising clustering an SSL session resumption between the first node and the one of the at least two SSL relays (see col.28, lines 41-55).

As per ***claim 36***, which depends on claim 28, Bruck teaches of further comprising clustering cryptographic keying information across all of the at least two SSL relays (see col.13, lines 40-44).

As per ***claim 39***, which depends on claim 36, Bruck does not teach of further comprising clustering a current key schedule (see col.13, lines 40-44).

As per ***claim 40***, which depends on claim 36, Bruck teaches of further comprising clustering a key and an offset into a key stream (see col.13, lines 40-44).

As per ***claim 42***, which depends on claim 28, Bruck teaches of further comprising clustering data from a partial record corresponding to data from either the first or second node (see col.24, lines 51-66).

As per ***claim 43***, which depends on claim 28, Bruck teaches of further comprising clustering an information size before the information is transmitted (implicit: see col.24, lines 53-55).

As per ***claim 47***, which depends on claim 46, Bruck does not teach wherein the (SSL) relay assumes the first SSL relay's responsibilities upon failure of the first SSL relay (see col.2, lines 49-54 & 63-65 and col.8, lines 62-65).

As per ***claims 51-54***, which depend on claim 49, Bruck further teaches wherein the first interface and the second interface and the third interface are the same (implicit: see col.5, line 51-col.6, line 4).

As per ***claims 55 and 62***, which depend on claims 28 and 46, respectively, Bruck teaches of further including the steps of:

clustering the transferred information in response to determining that the transferred information is a partial record (see col.10, lines 9-18: "*provides state sharing information among the all the machines in the cluster*" and col.24, lines 31-33: "*Consistent state sharing among the servers*"); and

transmitting a partial acknowledgment to the first node upon clustering the transferred information (see col.25, lines 1-8: "*for every packet received, the Reliable Message layer sends out an acknowledgment*").

As per ***claims 56 and 63***, which depend on claim 55 and 62, respectively, Bruck further teaches wherein the step of determining that transferred information is a partial record includes determining whether a packet interval timer has expired (see col.24, lines 57-58).

As per ***claims 57 and 64***, which depend on claim 28 and 46, respectively, Bruck teaches of further including the step of storing the transferred information in a queue until the second node has acknowledged the information (implicit: see col.24, lines 58-

63: "callback function to notify the upper layer software, passing it the record of the original message").

As per ***claim 60***, which depends on claim 44, Bruck further teaches wherein the handshake acknowledgement message includes at least one of a server handshake and a server handshake completion message (see col.25, line 64-col.26, line 2).

As per ***claim 61***, which depends on claim 60, Bruck further teaches wherein the first node is configured to transmit a key exchange message upon receiving the server handshake completion message (see col.13, lines 40-44).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 37, 38, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruck et al. (US 6,691,165 B1) in view of Weinstein et al. (US 6,094,485 A).

As per ***claim 37***, although Bruck teaches of further comprising clustering a key (see claim 36 rejection above), Bruck does not explicitly teach of clustering a current Cipher Block Chaining (CBC) residue.

Weinstein teaches of clustering a current Cipher Block Chaining (CBC) residue (see col.8, lines 5-10 and col.9, lines 24-28).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the teachings of Weinstein within the system of Bruck by implementing Cipher Block Chaining (CBC) residue within the method for clustered Secure Sockets Layer (SSL) acceleration because such implementation would provide a strong encryption scheme applicable with SSL.

As per ***claim 38***, Bruck does not explicitly teach of further comprising clustering a sequence number.

Weinstein teaches of further comprising clustering a sequence number (see col.9, lines 29-34).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the teachings of Weinstein within the system of Bruck by implementing clustering a sequence number within the method for clustered Secure Sockets Layer (SSL) acceleration because such implementation would provide a strong encryption scheme applicable with SSL.

As per ***claim 41***, Bruck does not explicitly teach of further comprising clustering a cipher state.

Weinstein teaches of clustering a cipher state (see col.11, lines 17-19).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the teachings of Weinstein within the system of Bruck by implementing clustering a cipher state within the method for clustered Secure Sockets

Layer (SSL) acceleration because such implementation would continue to provide transparent communication between the nodes even in the event of failure to one SSL relay.

As per ***claims 58 and 65***, which depend on claim 57 and 64, respectively, although Bruck further teaches wherein the transferred information is stored in the queue (implicit: see col.28, lines 23-28), Bruck does not explicitly teach of a cipher state associated with the information.

Weinstein teaches of cipher state associated with the information (see claim 41 rejection and motivation above).

As per ***claim 59***, which depends on claim 44, Bruck does not explicitly teach wherein the state information includes at least one of: a client random value, a server random value and a chosen cipher suite,

Weinstein teaches of state information includes at least one of a chosen cipher suite (see col.1, lines 50-63).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the teachings of Weinstein within the system of Bruck by implementing at least one of a chosen cipher suite within the system for clustered Secure Sockets Layer (SSL) acceleration because such implementation would provide a strong encryption scheme applicable with SSL.

Response to Arguments

8. Applicant's arguments filed May 30, 2006 have been fully considered but they are not persuasive.

A. Applicant argues with respect to claims 28 and 46 that Bruck fails to teach or suggest, "receiving an acknowledgment from the second node in response to determining that the transferred information is a full record".

Responsive to the above argument, it is noted that the limitation relied upon is not explicitly taught or supported by the specification. Page 16, lines 20-21 states, "When a full record has been ACKed, it may be removed from the list and a new state clustered". There is no teaching of "**determining** that the transferred information is a full record" (emphasis added). Even if such teachings is implied in the specification, there is no teaching whatsoever, suggesting that the acknowledgment is received "in **response** to" the determining step.

In fact, Bruck teaches the functionality taught by the applicant(s) as stated on page 16, lines 20-21. In column 24, lines 40-66, Bruck teach "*after all packets have been acknowledged by the receiver, the Reliable Message layer cleans the records for the packets and for the message by deletion*".

The applicant(s) seem to suggest that this is a novel feature of the invention, yet the specification fails to define what is a "full record".

Furthermore, the applicant(s) uses terminology "in response to", "upon", or the like wherein a functional reaction occurs based on some functional action, but does not show in the specification any support. These are explicit functional steps that are

claimed and must comply with a written description. Otherwise, the steps have no dependency upon the other steps and must be rewritten as such.

Example:

Claim 55. The method of claim 28, further including the steps of:

clustering the transferred information in response to determining that the transferred information is a partial record; and

transmitting a partial acknowledgment to the first node upon clustering the transferred information.

Should be re-written:

Claim 55. The method of claim 28, further including the steps of:

determining that the transferred information is a partial record;

clustering the transferred information; and

transmitting a partial acknowledgment to the first node.

B. The applicant(s) argue with respect to claim 44 that Bruck does not teach a "handshake". Bruck clearly teaches of a handshake. In column 25, line 64-col.26, line 2, Bruck teaches "connection between two machines are established following an exchange of messages including a synchronization segment message (SYN), acknowledgement message (ACK), and SYN-acknowledgement message (SYN-ACK)".

C. The applicant(s) argue with respect to claim 49, that Bruck does not teach, "wherein the acknowledgement is received in response to a determination that the

transferred information is a full record". See the response to argument regarding claims 28 and 46 above.

D. For the reasons above, the dependent claims remain rejected.

E. With respect to the argument regarding claims 37, 38, and 41, Weinstein is not relied upon to cure the above-mentioned deficiencies, because Bruck clearly and explicitly teaches the broad limitations.

Conclusion

9. For the reasons above claims 28-31 and 34-65 have been rejected and remain pending.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Y. Won whose telephone number is 571-272-3993. The examiner can normally be reached on M-Th: 7AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on 571-272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Michael Won

August 10, 2006